18.785: Analytic Number Theory, MIT, spring 2007 (K.S. Kedlaya)
A multiplicative large sieve inequality

In this unit, we convert the additive large sieve inequality from the previous unit, which concerned characters of the additive group, into a result about Dirichlet characters.

1 Review of the additive large sieve

The additive large sieve inequality from last time stated the following.

Theorem 1. *Fix $\delta \in (0, 1/2]$. Let $S \subset \mathbb{R}$ be a δ-spaced set (necessarily finite). Then for any $a_n \in \mathbb{C}$ for $M < n \leq M + N$,*

$$\sum_{\alpha \in S} \left| \sum_{M<n\leq M+N} a_n \exp(2\pi i \alpha n) \right|^2 \leq (\delta^{-1} + N - 1) \sum_{M<n\leq M+N} |a_n|^2.$$

We will need in particular the special case

$$S = \{a/q : 1 \leq q \leq Q, 0 \leq a < q, \gcd(a, q) = 1\}.$$

Note that if $a/q, a'/q' \in S$ are distinct and $m \in \mathbb{Z}$, then

$$\left| \frac{a}{q} - \frac{a'}{q'} - n \right| = \left| \frac{*}{qq'} \right| \geq Q^{-2}.$$

That is, S is δ-spaced for $\delta = Q^{-2}$. We thus obtain the following from the large sieve inequality.

Theorem 2. *Let N be a positive integer, and choose $a_n \in \mathbb{C}$ for $M < n \leq M + N$. Then*

$$\sum_{1\leq q\leq Q} \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left| \sum_{M<n\leq M+N} a_n \exp(2\pi i a n/q) \right|^2 \leq (Q^2 + N - 1) \sum_{M<n\leq M+N} |a_n|^2.$$

2 The Bombieri-Davenport inequality

We now ask the question: what if we replace the exponentials in the large sieve by the primitive Dirichlet characters of all moduli $q \leq Q$?

Theorem 3 (Bombieri-Davenport)**.** *Fix positive integers Q, N. For any $a_n \in \mathbb{C}$ for $M < n \leq M + N$, we have*

$$\sum_{1\leq q\leq Q} \frac{q}{\phi(q)} \sum_{\chi} \left| \sum_{M<n\leq M+N} a_n \chi(n) \right|^2 \leq (Q^2 + N - 1) \sum_{M<n\leq M+N} |a_n|^2. \qquad (1)$$

One can prove a stronger inequality in which you allow also some terms corresponding to imprimitive characters, but I won't need this.

Proof. As in the proof of the functional equation for Dirichlet L-functions, we use the expansion of primitive Dirichlet characters in terms of Gauss sums:

$$\chi(n) = \tau(\overline{\chi})^{-1} \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \overline{\chi}(a) \exp(2\pi i a n/q),$$

where

$$\tau(\chi) = \sum_{b \in \mathbb{Z}/q\mathbb{Z}} \chi(b) \exp(2\pi i b/q)$$

has the property that

$$|\tau(\chi)| = \sqrt{q}.$$

If we put

$$S(\alpha) = \sum_{M < n \leq M+N} a_n \exp(2\pi i \alpha n),$$

we can then write

$$\frac{q}{\phi(q)} \left| \sum_{M<n\leq M+N} a_n \chi(n) \right|^2 = \frac{1}{\phi(q)} \left| \sum_{a \in \mathbb{Z}/q\mathbb{Z}} \overline{\chi}(a) S(a/q) \right|^2.$$

Summing over $1 \leq q \leq Q$ and χ primitive gives the left side of (1). I can get an upper bound by summing over $1 \leq q \leq Q$ and *all* χ, primitive or not. By orthogonality of characters for the group $(\mathbb{Z}/q\mathbb{Z})^*$, this yields

$$\sum_{1 \leq q \leq Q} \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} |S(a/q)|^2 = \sum_{1 \leq q \leq Q} \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left| \sum_{M<m\leq M+N} a_n \exp(2\pi i a n/q) \right|^2$$

as an upper bound for the left side of (1). Applying Theorem 2 gives the right side of (1), completing the proof. □

3 An application of the large sieve

We will use the large sieve crucially in the Bombieri-Vinogradov theorem, but first let us illustrate its use with one of its original applications, due to Linnik.

The setup here is as in the sieve of Eratosthenes: I have a sequence of complex numbers a_n with finite support, a set of primes P, and for each $p \in P$, I wish to exclude a set of residue classes Ω_p of size $\omega(p)$. That is, I wish to compute Z, the sum of a_n over thoes n which do not reduce to a class in Ω_p for any $p \in P$. However, I'm not going to require $\omega(p)$ to be as small as I did before; that's what makes this a "large sieve".

Theorem 4. *Suppose the support of a_n belongs to an interval of length N, and that $\omega(p) < p$ for all $p \in P$. Let h be the multiplicative function with $h(q) = 0$ for q not squarefree and*

$$h(p) = \frac{\omega(p)}{p - \omega(p)}.$$

Then for any $Q \geq 1$,

$$|Z|^2 \leq \frac{N + Q^2}{H} \sum_n |a_n|^2,$$

where H is the sum of $h(q)$ over $q \leq Q$ squarefree. In particular, if $a_n \in \{0, 1\}$ for all n, then

$$Z \leq \frac{N + Q^2}{H}.$$

The proof will be immediate from Theorem 3 plus the following lemma (summed over q).

Lemma 5. *Put $S(\alpha) = \sum_n a_n \exp(2\pi i \alpha n)$. For any positive squarefree integer q,*

$$h(q)|S(0)|^2 \leq \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left| S\left(\frac{a}{q}\right) \right|^2.$$

Proof. We first reduce to the case where q is prime. Suppose $q = q_1 q_2$ and we know the desired result for both q_1 and q_2. By the Chinese remainder theorem,

$$\begin{aligned}
\sum_{a \in (\mathbb{Z}/q\mathbb{Z})^*} \left| S\left(\frac{a}{q}\right) \right|^2 &= \sum_{a_1 \in (\mathbb{Z}/q_1\mathbb{Z})^*} \sum_{a_2 \in (\mathbb{Z}/q_2\mathbb{Z})^*} \left| S\left(\frac{a_1}{q_1 + \frac{a_2}{q_2}}\right) \right|^2 \\
&\geq h(q_2) \sum_{a_1 \in (\mathbb{Z}/q_1\mathbb{Z})^*} \left| S\left(\frac{a_1}{q_1}\right) \right|^2 \\
&\geq h(q_1) h(q_2) |S(0)|^2 = h(q)|S(0)|^2.
\end{aligned}$$

It remains to prove the case where q is prime; we leave this case as an exercise. □

Here is Linnik's application of the large sieve. For p prime, let $q(p)$ be the least positive integer which is not a quadratic residue modulo p. It is conjectured that $q(p) = O(p^\epsilon)$ for any $\epsilon > 0$, but unconditionally this is only known for $\epsilon > e^{-1/2}/4 \cong 0.152$. On the other hand, under GRH, one can do much better: one proves $q(p) = O(\log^2 p)$.

Theorem 6 (Linnik)**.** *For any fixed $\epsilon > 0$, there exists $c = c(\epsilon)$ such that for any N, there are at most c primes $p \leq N$ such that $q(p) > N^\epsilon$.*

Proof. For convenience, we will prove instead that for some $c = c(\epsilon)$, for any N there are at most c primes $p \leq \sqrt{N}$ with $q(p) > N^\epsilon$. Let P be the set of primes $p \leq \sqrt{N}$ such that $\left(\frac{n}{p}\right) = 1$ for all $n \leq N^\epsilon$, and let Ω_p be the classes of quadratic nonresidues mod p. (This is indeed a large sieve, because $\omega(p) = (p-1)/2$, so $h(p) = (p-1)/(p+1) \sim 1/2$ as $p \to \infty$, whereas in our earlier examples $\omega(p)$ was bounded.)

We will now sieve on the set $\{1, \dots, N\}$, i.e., take $a_n = 1$ for $1 \leq n \leq N$ and $a_n = 0$ otherwise. The resulting sifted set includes all $n \leq N$ with no prime divisors greater than N^ϵ; if we let Z_ϵ be the number of these, then Theorem 4 applied with $Q = \sqrt{N}$ yields

$$Z_\epsilon \leq 2NH^{-1}.$$

On the other hand, if we let X_ϵ be the number of primes $p \leq \sqrt{N}$ with $q(p) > N^\epsilon$, then because $h(p) \geq 1/3$ for all p,

$$\frac{1}{3}X_\epsilon \leq \sum_{p \leq \sqrt{N}, q(p) \geq N^\epsilon} h(p) \leq H.$$

Hence $X_\epsilon Z_\epsilon \leq 6N$.

To conclude, we need to show that $Z_\epsilon \geq cN$ for some $c > 0$. In fact it can be shown that $Z_\epsilon \sim cN$ for some N, but as we don't care about the particular constant, it will suffice to exhibit a special class of numbers being counted by Z_ϵ which are sufficiently numerous. Namely, take $n = mp_1 \cdot p_k \leq N$ with $N^{\epsilon - \epsilon^2} < p_j < N^\epsilon$ for $j = 1, \dots, k = \epsilon^{-1}$; then

$$Z_\epsilon \geq \sum_{p_1, \dots, p_k} \left\lfloor \frac{N}{p_1 \cdots p_k} \right\rfloor \geq cN,$$

completing the proof. □

Exercises

1. Prove the following multivariate version of the additive large sieve inequality (but without optimizing the constant). Fix $\delta > 0$ and $d \geq 1$, and let $\alpha_i = (\alpha_{i,1}, \dots, \alpha_{i,d}) \in \mathbb{R}^d/\mathbb{Z}^d$ be points which are δ-spaced, in the sense that the distance from each $\alpha_{i,k} - \alpha_{j,k}$ to the nearest integer is at least δ (whenever $i \neq j$ and $1 \leq k \leq d$). Prove that there exists $c = c(d)$ (independent of δ and the α_i) such that for any $a_n \in \mathbb{C}$ with n running over $\{1, \dots, N\}^d$,

$$\sum_i \left| \sum_n a_n \exp(2\pi i (n \cdot \alpha_i)) \right|^2 \leq c(\delta^{-d} + N^d) \sum_n |a_n|^2.$$

2. Prove directly (by expanding the squares) that if we take take *all* characters, not just the primitive ones, of a single modulus q, then the large sieve inequality holds with the constant $q + N$. (This is not very useful in practice.)

3. Prove Lemma 5 in the case that q is prime. (Hint: there is no loss of generality in assuming that there is at most one n in each residue class modulo p, and none in the classes in Ω_p, such that $a_n \neq 0$. Then use orthogonality of characters on $\mathbb{Z}/q\mathbb{Z}$.)